Australian Government | acma

Australian Communications and Media Authority

communicating | facilitating | regulating

FACTsheet

Online social networking

Online social networking, or using web based services to connect and interact with people about shared activities or interests, can be a great way to pursue interests, establish and enhance existing friendships, play games, and share ideas.

While there are many benefits to interacting online, publishing too much personal information in an online personal profile, blog, or even chat, can be risky.

To reduce your risk online:

- Control who has access to your information
- Think carefully before you give away personal information (such as your name, age or email or postal address) or your financial details (especially credit card or bank account details)
- Set up and check online privacy and security settings when you create a personal profile to make sure you know who can access your information
- Know where you can go for help if you run into trouble or something goes wrong.

Being careless online can lead to damage to your reputation from unintended use of your personal information or become a victim of fraud, identity theft, scams, spam email messages and harassment (which includes cyberstalking and cyberbulling) and accidentally installing malicious software (malware) on your computer.

Damage to reputation

Information or photos posted to an online profile, blog or website can be used or taken out of context to embarrass you and damage your reputation. Cases have already occurred where employers have used publicly available profiles to fire staff and prosecutors have used information on profiles to win their cases in court.

You can minimise risks by taking some simple steps:

- Use security and privacy tools available in all reputable social networking sites to set your profile to 'private'.
- Do not include anything in your profile you do not want the world to know about you.
- Monitor your information and find out how to remove personal information and images you are not happy with.
- Remember that any information available about you online is potentially there forever. You can check what information about you is publicly available online by typing your own name into a search engine.

Online Fraud and Identity Theft

The more information you provide online, including social networking profiles, photos, posts and in live chats, the easier it is for criminals to use your details to steal your money or identity.

Limit personal information (such as birthdays, full names or surnames) you share online and before publishing any of your personal information, make sure you:

- Control who can see it.
- Use reputable sites.

Always remember that online contacts and connections may not be who they say they are.

Scams

Anyone can fall victim to criminals who pretend to be someone they are not in order to steal money. Scams work because they offer things people want (like a holiday, easy money or a date) for little effort or they scare people into believing they will lose money if they don't respond.

Requests for personal and financial information and offers of goods or prizes may come from strangers or even look like requests from 'friends'.

When using online social networking sites, don't respond to unexpected requests for personal or financial information. Inform your financial institution or report them to SCAMwatch.

You can find out more about common scams and report scams at www.scamwatch.gov.au or by calling 1300 302 502.

Spam

Spam is electronic 'junk mail' – unwanted messages, advertising products and services, sent to your email address or mobile phone.

Some spam promotes a product or invites you to visit a website. Other spam tries to scam or trick you into investing in fraudulent schemes or revealing your bank account or credit card details.

CANBERRA
Purple Building Benjamin Offices
Chan Street
Belconnen ACT 2617
PO Box 78
Belconnen ACT 2616
T: 02 6219 5555
F: 02 6219 5200

MELBOURNE
Level 44, Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC 3000
PO Box 13112 Law Courts
Melbourne VIC 8010
T: 03 9963 6800
F: 03 9963 6899

SYDNEY
Level 15, Tower 1 Darling Park
201 Sussex Street
Sydney NSW 2000
PO Box Q500
Queen Victoria Building NSW 1230
T: 02 9334 7700
F: 02 9334 7799

FACTsheet

An electronic message is spam if:

- It is unsolicited or sent without your consent.
- It does not contain accurate information about the sender of the message.
- It does not provide a way to unsubscribe from receiving more messages or it does not action an unsubscribe request within five working days.

To avoid spam:

- Check if your internet service provider has a spam filtering service.
- Use spam filtering software.
- Understand how your email address will be used before providing it online
- Check the terms and conditions of anything you sign up for. Are you consenting to receive commercial electronic messages?
- Do not respond if the email seems dubious. Never click on links in spam emails or buy spam-advertised products or services as many are fraudulent.
- If you are not sure if the message sender is genuine, contact SCAMwatch.
- If you know the message sender and you do not wish to receive further email, use the unsubscribe facility.
- If you receive a commercial electronic message to your mobile phone, reply with 'STOP'.

For more spam related information, including frequently asked questions or to report or make complaints about spam visit www.spam.acma.gov.au.

Harassment

When you online personal information is publicly available, people may use it to find ways to harass you or threaten you. The people may be known to you or may be anonymous.

Your best protection against harassment online is to control who can access your online information and not publish too much information to your social networking profile.

Always keep your physical address and location private. Think carefully about publishing names, photos showing car licence plates, street names and venues you frequent in a way that can be linked to you.

Malware

Malware, or malicious software, is a type of computer program that installs itself on your computer without your knowledge. The program is designed to collect sensitive information stored in your computer, such as your online banking password or credit card details. It will then use your internet connection to send this information to criminals who use it to steal from your bank account or commit fraud.

Malware is often installed by downloading files from unsecured sources or clicking on web links in emails or invitations which inadvertently lead to websites containing computer viruses or malicious content. The risk of downloading malware onto a computer you are using increases if you provide details in an unsecured online environment (such as a public computer or unsecured wireless connection).

To minimise the risks of downloading malware, make sure that you:

- Check your online social networking privacy settings. An open personal profile online means that strangers may be able to post files to your profile or links to malicious content
- Don't open attachments or click on links in emails unless you know they have come from a trusted source. If you're not sure, do not open the email until you have checked the source
- Are careful when giving permission for new social networking applications.
- Don't click on links in pop-up windows or to websites that you are not sure are trustworthy. They may redirect you to a website that automatically uploads malware
- Check your computer is protected by an active firewall and anti-virus software as it may not have been included when you purchased your computer
- Speak to your internet service provider about what it is being or can be done to secure your internet connection.

Looking after children online

Internet users are responsible for the amount of information they reveal online. Most information published online is available for anyone to view and may be difficult to remove. It can also be used for purposes that may not have been intended.

If you are supervising children using the internet, you can help them stay safe online by reminding them of the following simple steps:

- Never share passwords, no matter how much they trust their friends.
- Use strong passwords with a combination of letters and numbers, not something that is easy to guess, like a pet's name or a favourite singer.
- Don't publish their personal details or those of their friends, such as names, ages, school details, email addresses or phone numbers on social networking sites (including profiles).
- Don't publish inappropriate photos of themselves or anyone else and ask permission before writing about other people or publishing their photo.
- Don't reply to nasty email messages (but keep a copy of them in case they're needed if trouble arises).

FACTsheet

- Block senders of inappropriate or unpleasant messages or delete the person if they are in their contact list.
- Don't give out their mobile number to people they don't know or trust.
- Save all nasty messages on their email accounts or mobile phones as evidence and show an adult.

Contact the telecommunications company to block problem numbers on your mobile service.

For help and advice about kids' safety online contact the Cybersafety Contact Centre – 1800 990 176 or Kids Helpline on 1800 551 880.

For more detailed information on helping children stay safe online visit the ACMA site at www.acma.gov.au and the Cybersmart site at www.cybersmart.gov.au

Where to go for help

Most social networking sites have information and tools on how to report problems and help users control who can access their information. Check these out when you sign up and make sure you keep security and private settings up to date.

Report any criminal activity to the police in your state or territory.

ACCC www.accc.gov.au

For advice on scams and how to report them contact the Australian Competition and Consumer Commission (ACCC) or call SCAMwatch on 1300 302 502.

ACMA www.acma.gov.au

As well as information on how to help children stay safe online, the Australian Communications and Media Authority (the ACMA) has an internet hotline to report prohibited content at www.acma.gov.au/hotline or call 1800 880 176. Complaints about spam (e-mail, instant messages, SMS and MMS) can be made to the ACMA at www.spam.acma.gov.au

ASIC www.asic.gov.au

The Australian Securities and Investments Commission (ASIC) investigates scams involving financial products and services including cold calling, phone investment scams and illegal investment schemes.

Please note: this document is intended as a guide only and should not be relied on as legal advice or regarded as a substitute for legal advice in individual cases.

State and territory consumer affairs and fair trading agencies

State and Territory consumer affairs and fair trading agencies protect and promote the interests of consumers by providing advice and assistance, enforcing state consumer laws, investigating complaints, and resolving disputes.

NSW: Office of Fair Trading (OFT)
www.fairtrading.nsw.gov.au

VIC: Consumer Affairs Victoria (CAV)
www.consumer.vic.gov.au

QLD: Office of Fair Trading (OFT)

www.fairtrading.qld.gov.au

NT: Consumer Affairs (Department of Justice)
www.caba.nt.gov.au

SA: Office of Consumer & Business Affairs (OCBA)
www.ocba.sa.gov.au

WA: Department of Consumer and Employment Protection (DOCEP) www.docep.wa.gov.au

TAS: Consumer Affairs and Fair Trading (CAFT)
www.consumer.tas.gov.au

ACT: Office of Regulatory Services
www.ors.act.gov.au